

Umbra (UMB) — Livre blanc v0.1

Oct 1, 2026 · @S

Résumé

Umbra (UMB) est une monnaie numérique privée par défaut, conçue pour payer au quotidien aussi simplement qu'avec une carte. Elle réunit la confidentialité de Monero, une finalité visée sous la seconde et la possibilité pour chacun de créer sa propre crypto sur le réseau.

- **Rapide** : un bloc toutes les 30 secondes dès le lancement, quatre fois plus vite que Monero, et un paiement visible en une à deux secondes. La phase 2 vise une finalité sous la seconde, avec une preuve d'enjeu privée inspirée d'Alpenglow (Solana).
- **Votre propre crypto en quelques clics** : chacun peut créer sa crypto sur le réseau. Elle hérite de la confidentialité, de la vitesse et de l'échange intégré, et apparaît automatiquement dans tous les portefeuilles.
- **Privée par défaut** : montants, expéditeurs, destinataires et type d'actif sont cachés. Aucune porte dérobée, aucune clé maîtresse.
- **Lancement équitable** : environ un an de minage au processeur ouvert à tous, comme Monero, puis bascule vers une preuve d'enjeu privée, avec un staking sans minimum ni blocage.
- **Utile au quotidien** : encaissement par QR sans terminal, bouton de paiement à coller sur un site, codes partageables pour encaisser des UMB, séquestre avec un tiers qui confirme la transaction, premier paiement vers une adresse annulable 10 minutes, récupération sans phrase de 24 mots, héritage, sur ordinateur comme sur téléphone.
- **Ouverte sur les autres chaînes** : échanges atomiques intégrés avec XMR, BTC, LTC, DOGE, ETH (USDC, EURC) et SOL, sans plateforme centralisée.
- **Un prix qui se fixe tout seul** : chaque portefeuille calcule le cours de l'UMB à partir des échanges réglés sur la chaîne, médiane des prix horaires sur 30 jours glissants, sans remise à zéro ; chaque échange compté prouve son montant et paie 0,2 % de frais.
- **Un stablecoin par devise** : uEUR, uUSD, uJPY... sont intégrés au protocole à 1 unité de leur devise, pour les commerçants qui ne veulent pas de volatilité. Ils sortent d'une réserve que personne ne peut gonfler sans dépôt.

L'offre : une réserve de 1,2 M UMB déclarée au bloc 0, 21 M UMB émis en 10 ans, soit 22,2 M, puis 105 000 UMB par an pour la sécurité. Le code est open source. Ce document est un brouillon de travail, pas une offre d'investissement.

Le problème

Aujourd'hui, il faut choisir entre une monnaie rapide mais transparente, et une monnaie privée mais lente et peu pratique. Umbra refuse ce choix.

- **Transparence** : sur Bitcoin, Ethereum ou Solana, chaque paiement est public. Un employeur, un concurrent ou un escroc peut lire un solde, un salaire ou un prix fournisseur.
- **Lenteur** : Monero bloque les fonds reçus pendant 10 blocs, soit environ 20 minutes. Ethereum met [une douzaine de minutes](#) à rendre un paiement définitif.
- **Pas d'usage quotidien** : peu de monnaies privées proposent des tokens, un encaissement simple en magasin, une récupération de compte humaine ou un pont vers les autres chaînes.
- **Confiance abîmée** : prémines cachées, failles d'inflation invisibles et fonds d'équipe opaques ont entamé la réputation des monnaies privées.

Vision et principes

Umbra veut être l'argent liquide du numérique : privé comme des espèces, rapide comme une carte, juste dans sa distribution. Sept principes ne sont pas négociables.

1. **Vitesse** : chaque choix technique se juge au temps réel entre « envoyer » et « irréversible », preuve comprise.
2. **Confidentialité par défaut** : toutes les transactions sont privées. Aucun utilisateur n'a d'adresse publique.
3. **Zéro divulgation par un tiers** : ni porte dérobée, ni clé maîtresse, ni mécanisme permettant à quelqu'un d'autre de voir vos transactions. Seul le propriétaire peut prouver un fait précis (« solde $\geq X$ », « j'ai payé cette facture ») par une preuve à divulgation nulle de connaissance.
4. **Offre vérifiable** : l'émission et la réserve sont publiques et contrôlables par tous, même si les soldes restent cachés.
5. **Lancement équitable** : environ un an de minage au processeur, ouvert à tous dès le premier bloc. La seule allocation hors minage est la réserve de 1,2 M, déclarée dans ce document.
6. **Code ouvert** : tout est publié, compilable par chacun et audité avant le lancement.
7. **Aucune plateforme obligatoire** : on entre et on sort par des échanges atomiques de pair à pair, sans dépôt chez un tiers.

Architecture technique

Umbra démarre sur une base éprouvée, puis rejoint son architecture cible par mises à jour successives. La phase 1 reprend le code de Monero (licence BSD, en production depuis 2014) ; chaque brique suivante n'arrive qu'une fois auditée.

Brique	Phase 1 (lancement)	Architecture cible
Consensus	Minage au processeur (famille RandomX), un bloc toutes les 30 secondes	Preuve d'enjeu privée, vote BFT à la Alpenglow, finalité visée sous la seconde
Confidentialité de l'expéditeur	Signatures en anneau, comme Monero aujourd'hui	Preuve d'appartenance à toute la chaîne, sur le modèle de FCMP++
Montants et destinataires	Montants chiffrés, adresses furtives à usage unique	Idem, avec le type d'actif caché dans un pool unique
Tokens	UMB seul ; création de cryptos dès la phase 2	Actifs confidentiels émis par tous, dans le même ensemble anonyme
Réseau	Dandelion++, Tor et I2P	Mixnet intégré
Synchronisation	Nœuds distants, balises de vue	Détection « floue » sans clé de vue
Cryptographie	Courbes elliptiques classiques	Preuves à base de hachage et chiffrement post-quantique

Un seul ensemble anonyme. Chaque token émis sur Umbra circule dans le même pool que l'UMB, et un observateur ne sait même pas quel actif bouge. Plus il y a de tokens, plus chacun est anonyme.

La vitesse dès le lancement. En phase 1, un bloc part toutes les 30 secondes, quatre fois plus souvent que chez Monero. Un paiement apparaît chez le destinataire en une à deux secondes et reçoit sa première confirmation en 30 secondes en moyenne. Les fonds reçus redeviennent dépensables après 10 blocs, soit 5 minutes contre 20 chez Monero.

Sous la seconde en phase 2. Une finalité sous la seconde exige un consensus BFT à preuve d'enjeu, que le minage ne donne pas : d'où la bascule prévue après environ un an de minage, la même transition que Zano mène vers une preuve d'enjeu pure et privée. Celui d'Umbra s'inspirera d'[Alpenglow](#), la mise à jour de Solana qui vise 100 à 150 ms : un bloc devient définitif en un seul tour de vote quand 80 % de l'enjeu l'approuve, et les fonds sont redépensables aussitôt. Alpenglow est [encore en test public](#) : Umbra

reprendra ce qui aura fait ses preuves. Le vrai goulot sera le temps de preuve sur l'appareil ([Aztec annonce environ 2,5 s sur un ordinateur portable](#)) : l'objectif mesuré est la durée « envoi → irréversible », preuve comprise.

Staking privé. En phase 2, chacun peut staker sans minimum ni blocage et sans révéler son montant, sur le modèle de [Zarcanum chez Zano](#). Sans minimum, les petits détenteurs touchent eux aussi l'émission, qui sinon enrichirait surtout les gros. Les fonds encore dans les coffres de la réserve ne stakent pas et ne votent pas.

Comment fonctionne le staking (phase 2)

Staker, c'est simplement laisser son portefeuille ouvert. Chaque pièce non dépensée participe à un tirage au sort privé, avec une chance proportionnelle à son montant, sans que personne ne voie ni la pièce ni le montant.

1. **Le tirage privé produit les blocs.** À chaque créneau, le portefeuille calcule un ticket pour chacune de ses pièces : l'empreinte de sa clé à usage unique, du numéro de créneau et de l'aléa du réseau. La pièce gagne si ce ticket passe sous un seuil proportionnel à son montant. Le gagnant publie le bloc avec une preuve à divulgation nulle de connaissance : la pièce existe, n'est pas dépensée, lui appartient, et son montant caché franchit le seuil. Le réseau vérifie la preuve sans apprendre quelle pièce a gagné ni combien elle vaut. C'est le principe de Zarcanum, en service chez Zano.
2. **Un comité tiré au sort vote la finalité.** Le même tirage attribue, à chaque époque, des sièges de vote : de l'ordre de mille, qui pèsent tous pareil et se répartissent en proportion des montants. Chaque siège signe ses votes avec une clé propre au siège, jamais reliée à une pièce. Comme dans Alpenglow, un bloc devient définitif en un tour quand 80 % des sièges l'approuvent, ou en deux tours à 60 %. Ses fonds sont alors redépensables aussitôt.
3. **Les récompenses suivent les montants.** L'émission reste fixée par seconde (chapitre Économie) : le passage au staking ne change pas l'offre. Chaque bloc paie son producteur et les sièges qui ont voté, en sorties privées, avec les frais. Le gain attendu est proportionnel au montant : 1 UMB rapporte en moyenne, en proportion, autant que 100 000 UMB. Les petits montants gagnent plus rarement un bloc, mais les sièges, tirés bien plus souvent, lissent leurs gains.
4. **Sans blocage ni minimum.** Il n'y a ni dépôt, ni délai de retrait : une pièce dépensée quitte simplement le tirage. Seule condition : une pièce doit avoir un âge minimal (de l'ordre d'une heure) pour participer. Ainsi, personne ne peut fabriquer des pièces jusqu'à tomber sur un ticket gagnant.

5. **En ligne, ou par délégation.** Pour staker, le portefeuille doit être en ligne, car il signe avec les clés de ses pièces. Une délégation sans remise des fonds, avec une clé qui permet de staker mais pas de dépenser, est à l'étude.
6. **Sécurité.** Un bloc définitif ne se révise jamais. Un nœud qui rejoint le réseau part du dernier point définitif publié avec le logiciel, ce qui ferme les attaques « longue portée ». Un siège qui vote pour deux blocs concurrents se dénonce lui-même par ses deux signatures : ses votes sont ignorés et il perd ses récompenses de l'époque. Aucun fonds n'est confisqué, puisqu'aucun vote n'est relié à une pièce. Les hypothèses sont celles d'Alpenglow : jusqu'à 20 % d'enjeu malveillant et 20 % de plus simplement hors ligne. La taille du comité est choisie pour que la part de sièges d'un attaquant s'écarte très rarement de sa part d'enjeu ; ce calcul fait partie de l'audit. Les coffres de la réserve ne stakent pas et ne votent pas.
7. **Du minage au staking.** Après environ un an, une mise à jour ouvre une période hybride d'un mois : les mineurs produisent encore les blocs, et les stakeholders votent déjà leur finalité. Ensuite, les blocs ne viennent plus que du tirage privé. Si le staking n'est pas prêt et audité, le minage continue.

Paramètre	Cible, à calibrer sur le réseau de test	Ce qui la fixe
Créneau	1 à 2 s	le temps de preuve sur un ordinateur portable
Sièges du comité	environ 1 000 par époque	le hasard du tirage d'un côté, le trafic de votes de l'autre
Finalité	80 % en un tour, 60 % en deux	Alpenglow
Âge minimal d'une pièce	environ 1 h	empêcher de fabriquer des tickets
Partage de la récompense	à fixer	producteur du bloc et sièges votants

Rien de ce staking n'est encore dans le code : c'est la phase 2, avec sa propre recherche et son propre audit.

Créer sa propre crypto sur Umbra

Chacun peut créer sa propre crypto sur le réseau Umbra en quelques clics, sans écrire de code ni lancer de blockchain. Elle hérite aussitôt de la confidentialité, de la vitesse et de l'échange intégré d'Umbra. [Zano le fait déjà](#) avec des jetons privés : environ 750 y ont été

créés, pour 0,01 ZANO chacun.

1. **Créer** : dans le portefeuille, « Créer une crypto » demande un nom, un symbole, une offre (fixe, ou émission réservée au créateur), des décimales, un logo et une description.
2. **Enregistrer** : le réseau lui attribue un identifiant unique et publie son offre totale. Des frais de création en UMB, détruits, découragent le spam.
3. **Indexer** : elle apparaît automatiquement dans tous les portefeuilles, l'explorateur et le site. Chacun peut l'ajouter, la recevoir et payer avec.
4. **Coter** : elle s'échange aussitôt contre l'UMB par enchères groupées à chaque bloc (un seul prix par bloc, donc pas de front-running), et contre BTC, ETH ou SOL en passant par l'UMB. Son prix se calcule comme celui de l'UMB.

Mêmes garanties que l'UMB. Montants, adresses et même type d'actif restent cachés : un observateur ne sait pas quelle crypto circule, et chaque crypto grossit l'ensemble anonyme commun. Son offre reste vérifiable par tous : aucune unité ne peut apparaître hors des règles. Les frais d'une transaction se paient dans la crypto elle-même.

Pas d'imitations. Chaque symbole ne s'enregistre qu'une fois sur la chaîne, premier arrivé, et les codes des devises nationales (EUR, USD, GBP, JPY... environ 180), ainsi que tout symbole qui commence par l'un d'eux, sont réservés au protocole, comme les noms des grandes cryptos : impossible de créer un second « UMB » ou un faux « USDC ». Le portefeuille affiche toujours l'identifiant unique à côté du nom.

Exemples. Points de fidélité sans pistage, cartes cadeaux, billets numérotés (une offre de 1 donne un objet unique), monnaie locale, jeton d'une communauté, d'une association ou d'un projet.

La création de cryptos arrive en phase 2, avec la mise à jour multi-actifs de la couche de confidentialité, une fois audité.

Économie du UMB

L'offre atteint 22,2 M d'UMB à 10 ans, puis ne croît plus que de 105 000 UMB par an, soit moins de 0,5 % d'inflation, un taux qui baisse tout seul. Trois flux la composent.

Flux	Montant	Rythme	Bénéficiaire
Émission principale	21 000 000 UMB	En baisse régulière, nulle à 10 ans	Mineurs, puis validateurs
Émission de sécurité	105 000 UMB par an	À partir de la 10e année, à vie	Validateurs

Flux	Montant	Rythme	Bénéficiaire
Réserve	1 200 000 UMB	Créée au bloc 0	Voir ci-dessous

Les frais de transaction vont aux mineurs, puis aux validateurs. L'UMB se divise en 10 décimales : les 12 de Monero dépasseraient la capacité des compteurs 64 bits au-delà de 18,4 M d'UMB.

Une émission douce, sans halving. La récompense est fixée par seconde et non par bloc, pour survivre au passage en preuve d'enjeu. Elle baisse un peu à chaque bloc, de 4,2 M UMB par an au départ jusqu'à zéro la 10^e année :

$$r(t) = \frac{2 \times 21\,000\,000}{T} \left(1 - \frac{t}{T}\right), \quad \forall T = 10 \text{ ans}$$

Avec un bloc toutes les 30 secondes, cela fait environ 4 UMB par bloc au lancement, et 3,99 M UMB distribués aux mineurs la première année.

La réserve : déclarée, verrouillée, publique.

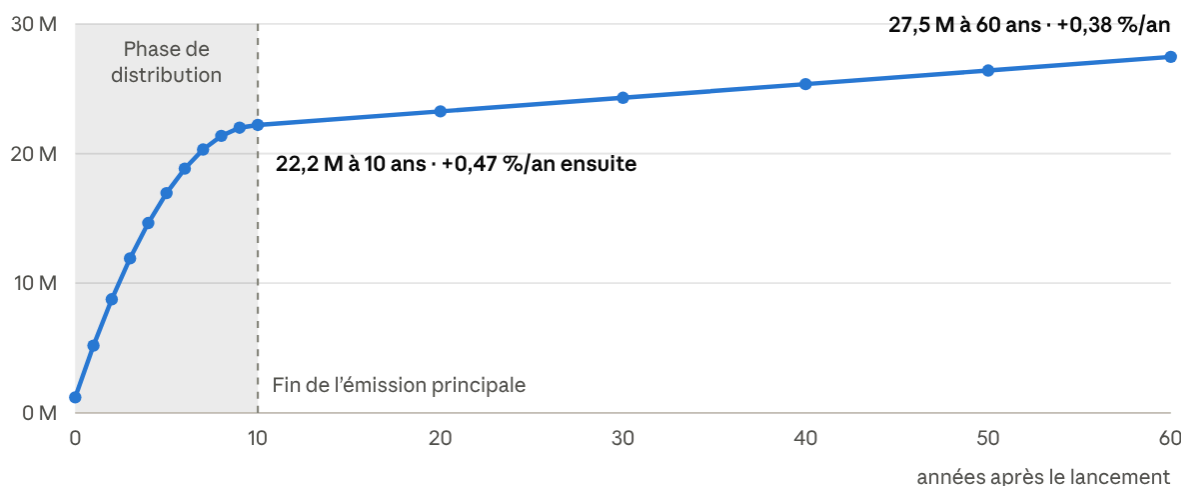
Poste	Montant	Déblocage
Développement	600 000 UMB	Immédiat, au bloc 0
Fonds de secours (piratages)	400 000 UMB	48 mensualités d'environ 8 333 UMB, dès le premier mois
Fondateur	200 000 UMB	Rien pendant 12 mois, puis 36 mensualités d'environ 5 556 UMB

- Le calendrier est écrit dans les règles de consensus : personne ne peut l'accélérer, pas même le fondateur.
- Les trois postes vont à une seule adresse de réserve. Elle est créée au bloc 0 en 85 sorties : une de 600 000 UMB utilisable aussitôt, et 84 mensualités verrouillées chacune jusqu'à sa hauteur de bloc. La clé de transaction du bloc 0 est publiée : chacun vérifie montants, adresse et dates dans l'explorateur.
- L'adresse de réserve est générée hors ligne par le fondateur ; seule sa partie publique figure dans le code. Une seule clé la contrôle, sans multisignature : elle doit rester sur un support déconnecté.
- La réserve pèse 5,4 % de l'offre à 10 ans. Une fois débloqués, les fonds entrent dans le pool privé : on voit le rythme, pas l'usage.

Trajectoire de l'offre.

L'offre atteint 22,2 M d'UMB à 10 ans, puis ne croît plus que de 105 000 par an

Offre totale en fin d'année, en millions d'UMB (réserve et émission principale incluses)



calculé à partir des paramètres ci-dessus · offre en fin d'année, années 0 à 60

Comme chez Monero, l'émission de queue compense les pièces perdues et paie la sécurité du réseau pour toujours, tandis que son poids relatif diminue chaque année.

Un prix qui se fixe tout seul

Personne ne fixe le prix de l'UMB. Chaque portefeuille le calcule lui-même à partir des échanges atomiques réglés sur la chaîne Umbra, et l'affiche dans l'application de bureau, l'application mobile et sur le site. Le même calcul donnera le prix de chaque crypto créée sur le réseau.

- 1. Un reçu dans la réclamation** : quand un échange pris sur une offre publique se règle, la transaction qui réclame les UMB porte un reçu. Il contient l'actif reçu en contrepartie, son montant, et le montant d'UMB avec de quoi ouvrir l'engagement du verrou : n'importe qui vérifie que le verrou contenait bien ces UMB. Aucune adresse n'y figure ; seul le montant de cet échange devient public.
- 2. Médiane des prix horaires sur 30 jours glissants** : chaque échange est converti en dollars au cours public de la monnaie de contrepartie (médiane de plusieurs sources ; USDC et EURC valent leur devise). Le prix d'une heure est la médiane de ses échanges, chacun comptant pour un. Le prix affiché est la médiane des prix horaires des 30 derniers jours, recalculée en continu, sans remise à zéro, en euros, en dollars et en BTC.
- 3. Prix 24 h pour les paiements** : un paiement libellé en euros ou dans une autre devise se convertit au prix des dernières 24 h, calculé de la même façon. Avec trop peu d'échanges, la période passe à 7 jours, puis à 30 jours.

4. **Pas de prix fragile** : avec moins de 50 échanges ou de 72 heures actives, la fenêtre s'allonge (60 jours, 120 jours...) au lieu de donner plus de poids à chaque échange. Avant le tout premier prix, l'application affiche « pas encore de prix ».
5. **Inscrit sur la chaîne en phase 2** : à chaque époque, les validateurs inscrivent ce même calcul et la chaîne retient la médiane de leurs résultats : personne ne choisit le prix. Il sert aux stablecoins nationaux et aux paiements libellés en devises.

Contre les échanges fictifs. Sur une chaîne privée, personne ne peut empêcher quelqu'un d'échanger avec lui-même. Ces règles font qu'un tel échange déplace à peine le prix et coûte de l'argent réel à son auteur. Les échanges qui ne les remplissent pas se font normalement, mais ne comptent pas dans le prix.

- **Montant prouvé** : un reçu qui n'ouvre pas l'engagement du verrou est ignoré.
- **0,2 % de frais** : la réclamation qui porte le reçu paie au moins 0,2 % du montant d'UMB aux mineurs. Chaque échange truqué coûte donc une part de sa taille.
- **Au moins 1 UMB** : les miettes ne comptent pas.
- **Un échange, une voix** : la taille d'un échange ne lui donne pas plus de poids dans son heure, et aucune heure ne pèse plus qu'une autre.
- **Stablecoins exclus** : les échanges contre les stablecoins d'Umbra ne comptent pas, puisque leur prix découle de celui-ci.

Pour déplacer le prix malgré tout, il faudrait posséder la majorité des échanges dans la majorité des heures actives du mois, en payant chaque fois 0,2 % : un coût qui grandit avec l'activité réelle. Les tests du code le vérifient : 100 échanges à trois fois le prix le déplacent de moins de 5 %, et il faut dominer plus de 400 heures pour le faire bouger. Aucun prix décentralisé n'est invulnérable ; celui-ci est coûteux à truquer, et ce coût se mesure. Le montant payé sur l'autre chaîne ne se prouve pas depuis Umbra : chaque portefeuille le vérifie pour ses propres échanges, et la médiane sur des centaines d'heures défend le reste.

Transparence sur la liquidité. Les applications affichent, à côté du prix sur 30 jours, le prix des dernières 24 h et le nombre d'échanges retenus. Toutes les chaînes d'échange sont prêtes sur le réseau de test, pour que le prix existe dès le lancement. Les reçus sont écrits par défaut pour les échanges pris sur une offre publique, et désactivables.

Fonctionnalités

Umbra réunit dans un seul portefeuille ce qui est aujourd'hui dispersé entre plusieurs applications. Chaque fonction respecte la règle de base : rien n'est visible par un tiers.

Échanges atomiques intégrés. Le portefeuille échange l'UMB de pair à pair, sans plateforme ni jeton intermédiaire. Les chaînes se regroupent en quatre modules :

Module	Chaînes couvertes	Remarque
Monero	XMR	Umbra joue le rôle de Bitcoin : ses verrous natifs (approbation, réclamation forcée, remboursement qui révèle une part de clé) sécurisent l'échange. Testé contre Monero v0.18.5.1 officiel, dans les deux sens et en cas d'abandon.
Famille Bitcoin	BTC, LTC, DOGE	Taproot (BTC, LTC) et P2SH (DOGE), avec signatures adaptatrices. BTC (Bitcoin Core), LTC et DOGE testés dans les deux sens.
EVM	ETH, ses couches 2, USDC, USDT et EURC	Un seul contrat pour ETH et tout jeton ERC-20 ; ETH et un jeton à 6 décimales testés, remboursements compris. Sans ETH pour le gaz, un relais réclame à la place du vendeur et se paie dans le jeton échangé.
Solana	SOL, USDC et EURC	Un seul programme pour SOL et tout jeton SPL (USDC, EURC) ; SOL et USDC testés dans les deux sens, remboursements et refus compris.

- Umbra ajoute les verrous temporels natifs dont Monero est dépourvu, pour échanger dans les deux sens.
- Signatures adaptatrices plutôt que HTLC : aucun hash commun ne relie les deux chaînes.
- Un échange attend les confirmations des deux chaînes, [soit des dizaines de minutes](#) côté Bitcoin ; Lightning rend l'échange instantané côté BTC et LTC.
- Des teneurs de marché fixent leur taux ; un dépôt de garantie décourage l'« option gratuite » (abandonner l'échange si le prix bouge).
- L'échange est intégré au paiement : on paie en BTC, le marchand reçoit en UMB ou dans le stablecoin de sa devise, et les frais sont payables dans n'importe quel token. Sur Ethereum, celui qui reçoit des USDC sans posséder d'ETH n'en achète pas : un relais soumet la réclamation et se paie dans le jeton échangé, aux frais inscrits dans le verrou (trois fois le minimum des relais, toujours sous 10 % du montant). Il ne peut ni détourner les fonds ni augmenter ses frais.
- Chaque échange réglé qui respecte les règles anti-fraude alimente le prix du UMB (section précédente).

Stablecoins nationaux. Chaque devise nationale a son stablecoin intégré au protocole : uEUR, uUSD, uGBP, uJPY... Leur valeur est inscrite dans le code : 1 uEUR = 1 €, 1 uUSD = 1 \$. Le protocole vend chacun contre son équivalent en UMB et le rachète au même taux, à tout moment. Entre deux stablecoins, l'échange suit le taux de change officiel, médiane de plusieurs sources publiques, et le portefeuille propose d'office la devise du pays de l'utilisateur.

Une réserve, pas une planche à billets. Personne n'émet les stablecoins, pas même l'adresse de développement : chacun en achète autant qu'il veut en convertissant des UMB au prix du moment, et les revend de la même façon. Les UMB versés restent bloqués dans une réserve tenue par le protocole. Personne ne peut les retirer : ils servent uniquement à racheter les stablecoins à leur valeur.

Le coussin. Si l'UMB perd 50 %, une réserve qui valait exactement les stablecoins émis n'en couvre plus que la moitié, et le stablecoin décroche : c'est ce qui a fait tomber [TerraUSD en mai 2022](#), avec près de 45 milliards de dollars effacés en une semaine. Tant que la réserve vaut au moins 4 fois les stablecoins en circulation, l'achat est donc illimité ; en dessous, il se met en pause, et le rachat reste toujours ouvert. Le coussin vient de l'adresse de développement au départ (par exemple 100 000 UMB sur les 600 000), des frais de conversion qui restent dans la réserve, et d'apporteurs qui déposent des UMB contre une part de ces frais. Ils peuvent retirer leur part tant que la réserve reste au-dessus de 8 fois la circulation.

Les conversions se font au prix de l'heure suivante, pour qu'un prix en retard ne puisse pas être exploité. Les stablecoins arrivent en phase 4, après audit et avis juridique.

Messagerie entre adresses. Messages chiffrés de bout en bout, hors chaîne, acheminés par le réseau anonyme. On y joint une facture, un reçu, une preuve de paiement ou une preuve « solde ≥ X » liée au destinataire, impossible à rejouer.

Codes partageables. Un montant verrouillé sur un code secret, partagé en QR, par SMS ou par message : qui le saisit encaisse les fonds.

- Expiration avec remboursement automatique au créateur, PIN optionnel envoyé à part.
- L'acheteur réclame le code sur place avant de payer, ce qui empêche la double vente.
- Usages : cadeaux, envoi à quelqu'un sans portefeuille, revente de codes par des tiers, qui portent leur propre statut réglementaire.

Séquestre : un tiers qui confirme. Pour les ventes entre particuliers, les fonds restent dans un coffre à trois clés (acheteur, vendeur, tiers choisi à deux) : deux accords suffisent pour libérer ou rembourser, et le tiers ne tranche qu'en cas de litige. L'option « annulable 10 minutes » vers un nouveau contact protège des arnaques et des fautes de frappe.

Récupération « 2 sur 3 ». Trois éléments, deux suffisent : le téléphone (biométrie), un kit de secours (carte QR imprimée et phrase de 5 mots retenue) et des proches (2 sur 3) qui ne voient rien seuls. Un mode expert affiche aussi la clé en 16 mots, date de création incluse.

Héritage. Si le compte dort X mois, une transaction pré-signée confiée à des relais transfère les fonds à l'héritier. Le portefeuille la renouvelle à chaque activité.

Export comptable signé. Le portefeuille produit un relevé signé, dont chaque ligne est prouvée sur la chaîne et qui contient l'empreinte du relevé précédent. Un identifiant de déclaration, jamais publié sur la chaîne ni dans un QR, rend visible un changement de portefeuille. Il sert aux impôts et à justifier l'origine des fonds auprès d'une banque.

Vie courante. Loyers et abonnements planifiés par le portefeuille, cagnottes, partage de dépenses entre colocataires.

Paiement annulable. Un premier paiement vers une adresse reste annulable 10 minutes. Il est vérifié tout de suite et les fonds qu'il utilise lui sont réservés, mais il ne part qu'à la fin du délai : d'ici là, « Annuler » le supprime et rien n'a quitté l'appareil. Au départ, il est signé à partir des mêmes fonds, avec des membres de cercle et des frais du moment ; il ne peut jamais partir deux fois. Cela protège d'une adresse mal copiée, ou remplacée par un logiciel malveillant dans le presse-papiers.

Commerçants : QR et bouton de paiement

Un commerçant encaisse avec son seul téléphone ou son site, sans terminal ni prestataire de paiement. Cible prioritaire : freelances, commerçants et PME, pour qui la confidentialité des prix et des salaires devient un argument commercial. Deux outils suffisent.

Encaisser en face à face.

1. Le vendeur appuie sur « Encaisser » et tape le montant, en UMB ou dans sa devise, converti au prix des dernières 24 h.
2. Un QR apparaît, avec une adresse à usage unique propre à cette vente.
3. L'acheteur scanne et paie ; « Payé » s'affiche sur les deux écrans.

En phase 1, le paiement apparaît en une à deux secondes et reçoit sa première confirmation en 30 secondes en moyenne ; en phase 2, il devient définitif en moins d'une seconde. Un QR fixe imprimé convient aux stands (l'acheteur tape le montant), un lien de paiement aux ventes à distance, et le reçu part tout seul par la messagerie.

Un bouton de paiement à coller sur son site. Dans le portefeuille, « Mode vendeur → Bouton de paiement » génère un court extrait de code à coller sur n'importe quel site.

```
<script src="https://umbra.example/pay.js"
  data-address="ADRESSE_PUBLIQUE_DU_VENDEUR"
  data-amount="12.5" data-currency="UMB"
  data-label="Commande 1042"></script>
```

- Le bouton ouvre une fenêtre avec le montant, le QR et une référence unique par commande.
- Chaque commande reçoit sa propre adresse intégrée, calculée dans le navigateur à partir de l'adresse publique du vendeur : aucun secret n'est exposé.
- Les petits vendeurs voient les paiements arriver dans leur portefeuille, avec le numéro de commande.
- Pour valider une commande automatiquement, un petit serveur « Umbra Pay » auto-hébergé surveille les paiements avec la clé de réception du vendeur, sur le modèle de BTCPay Server, puis prévient la boutique.
- Extensions prévues pour WooCommerce, Shopify et PrestaShop.

Le montant peut être fixé en UMB ou en euros : le bouton convertit au prix des dernières 24 h, publié par les nœuds publics. Dès la phase 4, un commerçant qui ne veut pas de volatilité reçoit directement le stablecoin de sa devise.

Applications

Umbra arrive d'abord comme un portefeuille de bureau pour Windows, macOS et Linux, qui sait aussi miner. Le téléphone suit avec un portefeuille léger, sans minage.

Ordinateur. Une interface graphique unique, simple par défaut :

- Mode simple par défaut : aucun téléchargement de la chaîne, connexion à un nœud distant.
- Mode avancé : nœud complet ou élagué, qui démarre tout de suite sur un nœud distant pendant sa propre synchronisation.
- Onglet Minage : un bouton pour miner avec le processeur, choix du nombre de cœurs, minage en solo ou en pool.
- Le prix du UMB s'affiche en permanence ; mode vendeur, codes, messagerie et échanges arrivent au fil des phases.

Les versions Windows et macOS sont compilées automatiquement par intégration continue. Leur signature (certificat Windows, notariation Apple, qui exige un compte développeur payant) évite les alertes au téléchargement.

Outils de minage.

- Mineur intégré au portefeuille, pour le processeur.

- XMRig, le mineur en ligne de commande le plus répandu, adapté à Umbra (algorithme rx/umb, reconnu à l'adresse, minage en solo contre un nœud, testé) pour les serveurs et petites fermes, sous Windows, macOS (Intel et Apple Silicon) et Linux.
- Une pool décentralisée sur le modèle de P2Pool, pour ne dépendre d'aucune pool centrale.
- Des guides : pages mémoire étendues, réglage des cœurs, consommation électrique.

En phase 2, le staking privé remplace le minage, depuis le même portefeuille.

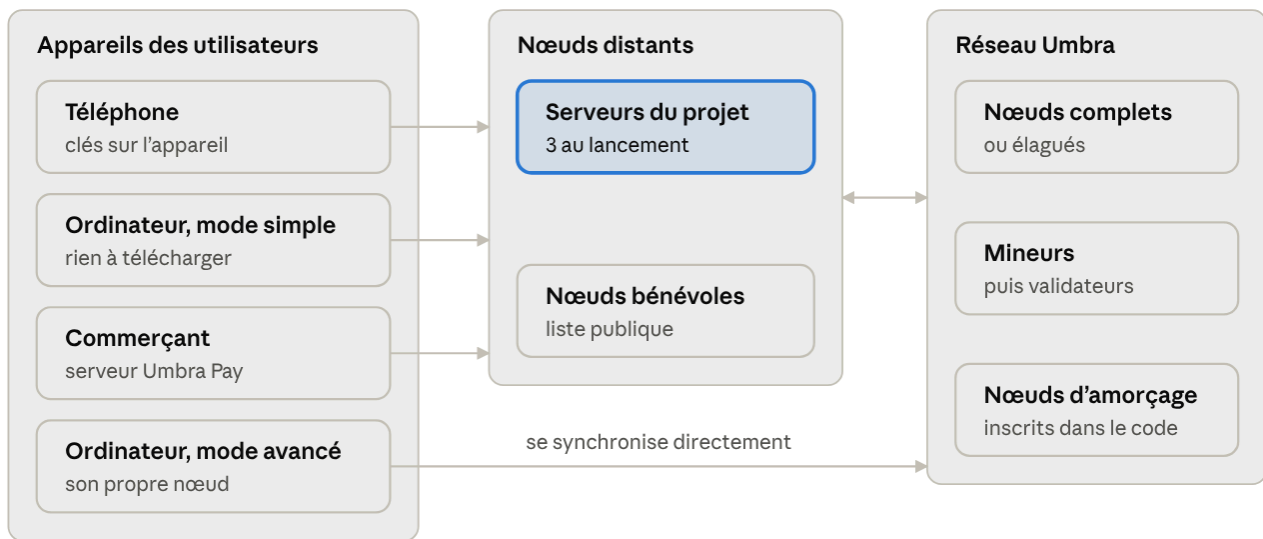
Téléphone : la proposition.

1. Un portefeuille léger, prêt sur le réseau de test : une application installable depuis le navigateur du téléphone (français, anglais), emballée pour Android et iOS. Le téléphone ne stocke pas la chaîne : il lit les blocs d'un nœud et retrouve ses paiements lui-même. Il choisit les membres de cercle, calcule les frais et signe comme le portefeuille de bureau, si bien que ses transactions ne se distinguent pas sur la chaîne. Les clés ne quittent jamais l'appareil ; elles y sont chiffrées (mot de passe d'au moins 10 caractères, 600 000 tours de PBKDF2) et l'écran se verrouille seul.
2. À court terme, viser l'intégration dans un portefeuille multi-devises existant : [Zano a noué ce partenariat avec Cake Wallet](#).
3. Pas de minage sur téléphone : batterie, chauffe, et les boutiques d'Apple et de Google interdisent le minage sur l'appareil.
4. Distribution par Google Play, l'App Store, F-Droid et un fichier APK direct.

Noeuds et infrastructure

Personne n'a besoin de télécharger toute la chaîne pour utiliser Umbra : portefeuilles de bureau et mobiles se connectent par défaut à des nœuds distants. Les clés restent sur l'appareil ; le nœud ne fait que servir les blocs.

Seuls les blocs voyagent : les clés restent sur l'appareil



architecture des nœuds au lancement

Téléphones, ordinateurs en mode simple et serveurs de commerçants interrogent des nœuds distants ; seul un ordinateur en mode avancé télécharge la chaîne et rejoint directement le réseau.

Mode	Espace disque	Pour qui
Nœud distant (par défaut)	Aucun	Téléphone, débutants
Nœud élagué	Environ un tiers de la chaîne	Ordinateur, confidentialité renforcée
Nœud complet	Toute la chaîne	Mineurs, commerçants, opérateurs de nœuds

Faut-il acheter des serveurs ? Oui, trois au lancement.

- Chacun joue deux rôles : nœud d'amorçage, inscrit dans le code pour que les nouveaux nœuds trouvent le réseau, et nœud distant public en mode restreint, pour les portefeuilles légers. Ils servent aussi le prix du UMB au site et au bouton de paiement.
- Répartis chez au moins deux hébergeurs et dans deux pays, pour qu'une panne ou une pression n'arrête pas tout.
- Budget : trois petits serveurs CX33 chez Hetzner coûtent [environ 25 € par mois](#), après [la hausse de 30 à 40 % de juin 2026](#).
- La chaîne restera petite les premières années : un disque de 80 à 160 Go suffit au départ, à agrandir avec l'usage.

- Une adresse unique du type nodes.<domaine du projet> répartit les portefeuilles entre les serveurs ; la liste des nœuds est publiée et le portefeuille en choisit un au hasard.

Ensuite, la communauté prend le relais : liste publique de nœuds bénévoles, installation en une commande, puis validateurs servant aussi de nœuds en phase 2. Les serveurs du projet ne doivent jamais être les seuls, sinon ils deviennent un point de pression.

Gouvernance, transparence et sécurité

La confiance dans Umbra repose sur ce que chacun peut vérifier, pas sur des promesses. Sur une chaîne privée, une faille d'inflation reste invisible : [Zano a dû effacer 30 jours d'historique en septembre 2026](#) après une telle faille.

- Code source public dès le premier jour, sous licence BSD héritée de Monero.
- Compilations reproductibles : chacun vérifie que les exécutables correspondent au code.
- Audit indépendant de la cryptographie et du consensus avant le lancement, puis à chaque mise à jour majeure.
- Programme de récompense pour les failles dès le testnet.
- Testnet public d'au moins trois mois avant le lancement.
- Réserve publique, calendrier de vesting inscrit dans le consensus.
- Évolutions proposées et discutées publiquement avant chaque mise à jour du réseau ; en phase 2, les stakers votent, hors fonds de la réserve.

Cadre réglementaire

Umbra sera légal à détenir mais absent des plateformes régulées, en Europe comme ailleurs. Le projet s'organise pour ne pas en dépendre.

- **Union européenne** : à partir du 10 juillet 2027, le règlement AMLR interdit aux plateformes régulées de lister ou conserver des cryptos anonymisantes, même quand la confidentialité est optionnelle. Les particuliers peuvent toujours en détenir ([source](#)).
- **Hors UE** : Dubaï, le Japon et la Corée du Sud interdisent déjà ces cryptos aux plateformes régulées ; à mi-2026, aucun pays ne pénalise la simple détention de Monero ([source](#)).
- **Conséquence** : distribution par échanges atomiques de pair à pair et par codes partageables, sans plateforme centralisée.

- **Stablecoins nationaux** : dans l'UE, un jeton qui vise la valeur d'une seule devise officielle est un « jeton de monnaie électronique », que seul un établissement de crédit ou de monnaie électronique agréé peut offrir au public ([règlement MiCA, articles 3 et 48](#)). Dans Umbra, aucune clé n'émet ces jetons : la réserve gérée par le protocole réduit ce risque sans le supprimer, et un avis d'avocat est indispensable avant leur activation.
- **Tiers** : créateurs de cryptos, revendeurs de codes, tiers de séquestre, opérateurs de services et teneurs de marché portent leur propre statut réglementaire ; un jeton adossé à un actif ou un titre financier créé sur Umbra peut relever de MiCA ou du droit financier.
- **Offre au public** : vendre des jetons au public dans l'UE peut exiger un livre blanc conforme au règlement MiCA ; ce document n'en est pas un. Le minage et les distributions gratuites en sont en principe exemptés.

Ce chapitre n'est pas un avis juridique : il doit être validé par un avocat spécialisé avant tout lancement.

Risques et limites

Le plus grand risque est le lancement lui-même : une petite chaîne minée au processeur peut être dominée par une fraction de la puissance de Monero. Voici chaque risque identifié et sa parade.

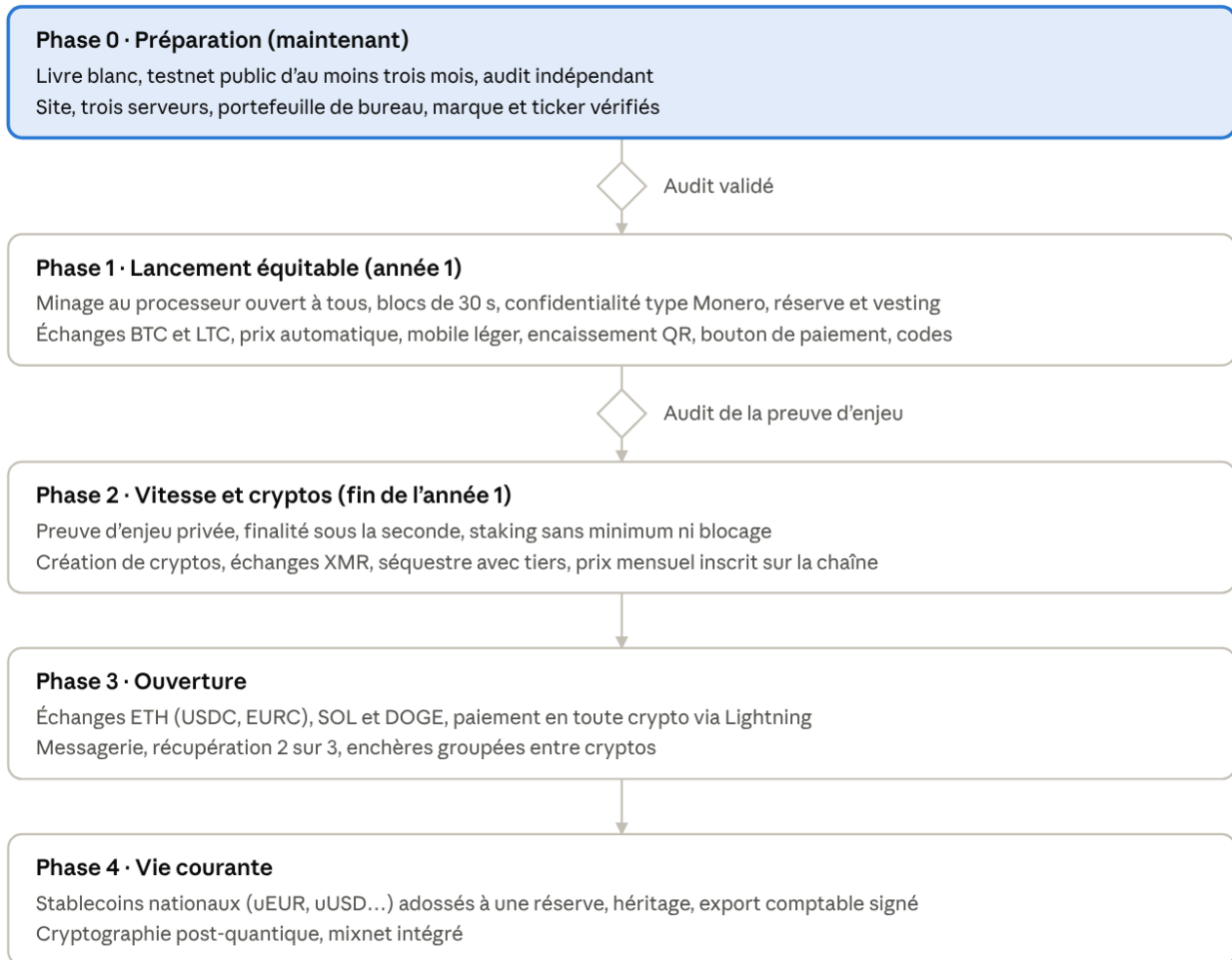
Risque	Conséquence	Parade
Attaque à 51 % pendant le minage	Réorganisation de blocs, double dépense ; même Monero a subi une réorganisation de 18 blocs en septembre 2025	Variante dédiée de l'algorithme, points de contrôle publiés pendant la phase 1, ou minage fusionné avec Monero comme Tari
Faillie cryptographique ou d'inflation	Création de monnaie invisible	Audits, testnet long, offre vérifiable, récompense pour les failles
Bascule en preuve d'enjeu retardée	Pas de finalité sous la seconde	Les blocs de 30 secondes continuent tant que la phase 2 n'est pas audité
Blocs de 30 secondes	Plus de blocs orphelins, chaîne plus lourde	Propagation compacte des blocs, nœuds élagués

Risque	Conséquence	Parade
Manipulation du prix	Cours faussé par des échanges fictifs	Seuls comptent les échanges réglés sur la chaîne, chacun prouvant son montant d'UMB et payant 0,2 % de frais ; médiane des prix horaires sur 30 jours, une voix par échange
Cryptos frauduleuses ou imitations	Faux « USDC », arnaques à l'émission	Symboles uniques ; codes des devises nationales et tout symbole qui commence par l'un d'eux réservés au protocole ; identifiant affiché partout
Clé unique de la réserve	Vol ou perte des tranches futures	Clé générée et conservée hors ligne
Nom et ticker déjà utilisés	Confusion, litige de marque	« Umbra » désigne déjà deux protocoles de confidentialité (Ethereum , Solana) et UMB le jeton d' Umbrella Network : vérifier la marque, changer de ticker si besoin
Réglementation	Absence des plateformes régulées	Distribution de pair à pair, avocat spécialisé
Stablecoins nationaux	Parité perdue si l'UMB s'effondre ou si un prix en retard est exploité ; statut de monnaie électronique (MiCA)	Personne n'émet : achat illimité tant que la réserve vaut 4 fois la circulation, en pause en dessous, rachat toujours ouvert ; conversions au prix de l'heure suivante ; avis d'avocat avant activation
Temps de preuve sur téléphone	Paiement plus lent que visé	Mesurer « envoi → irréversible », optimiser les preuves

Feuille de route

Umbra avance en cinq phases, chacune ouverte seulement une fois la précédente auditée.

Rien ne passe en production sans audit : cinq phases, du testnet à la vie courante



feuille de route · 5 phases, 2 audits bloquants

Les dates restent indicatives : si la preuve d'enjeu n'est pas prête et auditée, le minage continue.

Références

- [Tatum – Alpenglow, finalité en un tour à 80 % de l'enjeu](#)
- [CryptoDaily – Alpenglow en test public, objectif 150 ms](#)
- [Cointelegraph – finalité d'Ethereum et de Solana](#)
- [The Defiant – temps de preuve d'Aztec](#)
- [TokenPost – stressnet FCMP++ de Monero](#)
- [Zano – présentation et staking privé Zarcantum](#)
- [Zano – Zenith, passage à une preuve d'enjeu pure](#)
- [StealthEX – AMA Zano, actifs confidentiels](#)
- [ChainCatcher – retour arrière de 30 jours de Zano](#)

- [BasicSwap – paires supportées](#) et [FAQ](#)
- [eigenwallet – échanges atomiques BTC→XMR](#)
- [MoneroSwap – échanges EVM→XMR](#)
- [CryptoDaily – Zano et Cake Wallet](#)
- [Northflank – tarifs Hetzner 2026](#) et [CostGoat](#)
- [The Crypto Times – AMLR](#)
- [Monerica – légalité de Monero par pays](#)
- [CoinCentral – réorganisation de 18 blocs sur Monero](#)
- [The Block – minage fusionné de Tari](#)
- [ScopeLift – Umbra sur Ethereum](#), [Umbra Privacy sur Solana](#), [Solana Compass – Umbrella Network \(UMB\)](#)